Solution Architecture Description AMC

AMC 3 with AMC Controller 2.0

Aastra Deutschland GmbH
Zeughofstraße 1
10997 Berlin • Germany

AMC 3 with AMC Controller Solution document content:

1 Introduction 3
2 Overview Description AMC 3 & AMC Controller 2.0 3
3 AMC Controller 2.0 5
3.1 Architecture 5
3.2 AMCC Server 5
3.3 AMCC 2.0 Server Requirements WLAN 6
3.4 AMCC Capacity Options (SME) 6
4 AMCC Manager Features 6
5 AMC 3 Features 6
6 AMCC Key Features 7
7 Deployment 8
7.1 Installation and Configuration 8
7.2 Communication System Integration 8
7.3 AMC 3 Provisioning 8
8 Operation and Maintenance 8
9 Additional Features 9
9.1 High Availability 9
9.1.1 Linux HA-based Failover 9
9.1.2 General Information 9
9.2 AMC 3 Security 9
9.2.1 AMC Controller Security Options 10
9.2.2 Security Guidelines 10
9.3 AMCC Unified Communication Functions 11
9.3.1 AMC Corporate Phonebook 11
9.3.2 AMC Instant Message & Presence 11

1 Introduction

Aastra Mobile Client (AMC) solution is designed to work with all Aastra communications platforms. The Aastra Mobile Client 3 version (AMC 3) requires the AMC Controller (AMCC). The AMC Controller connects the AMC 3 to the Aastra communications platforms via SIP user interface. AMC Controller supports the following features & functions:

- Mobile integration over SIP
- Dual-Mode (WLAN / mobile network)
- Directory Search / LDAP
- Least Cost Routing
- trueCLIP
- Mobile Presence & Instant messaging (IM)
- Encrypted VoIP (SRTP)

This document provides a description of the AMC 3 in connection with the AMC Controller for mobile SIP integration with dual mode and Unified Communications features.
It includes a description of the system components and functions, different configurations and the applicable management functions.

2 Overview Description AMC 3 & AMC Controller 2.0

The AMC 3 and AMC Controller 2.0 solution is a client-server based solution offering mobile phone integration over SIP as well as seamless call continuity when the user moves back and forth between cellular (2G/3G) and WLAN networks.

The SIP-based AMC 3 installed on a Smartphone - supporting connections to both cellular and WLAN (802.11) networks in parallel - interacts with the communications system through the AMCC. The AMC 3 and the AMCC jointly manage the call and perform the handover seamlessly between the alternative networks. Handover from GSM to WLAN is initiated automatically but is transparent for the user. The handover from WLAN to GSM has to be done manually on the iPhone. 1

The AMC 3 runs on Black Berry 6.0 - 7.0, iPhones (Apple) higher than 3GS & Android 2.3 and 4.x. Please see *Supported Device Portal AMC* on Aastra InfoChannel in order to get more information about recommended mobile phone OS types and versions. Devices not listed there are generally not supported.

Once the AMC 3 users are configured via the AMC portal & the AMCC management GUI, the AMCC manages the user registration on the Aastra communications system and keeps track of the users' presence on the network. Together with the AMC 3 the AMCC also manages central and communications system related parts of the handover activity. The call setup to and from the Public Land Mobile Network (PLMN) is done through the communications system where the public trunk interface is converted to and from a SIP network interface to the AMCC. The AMCC also converts DTMF tones received (requests for telephony services generated from the AMC 3, e.g. on only-2G-connection) to SIP info messages that can be handled by the communications system. The AMCC

[1] iPhone does not support automatic handover from WLAN to GSM, only from GSM to WLAN.

solution also supports corporate phonebook access over LDAP and Instant Message & Presence Federation over XMPP, if the company has set up a compatible server (IM requires a 3rd Party XMPP-Server – e.g. “OpenFire”).

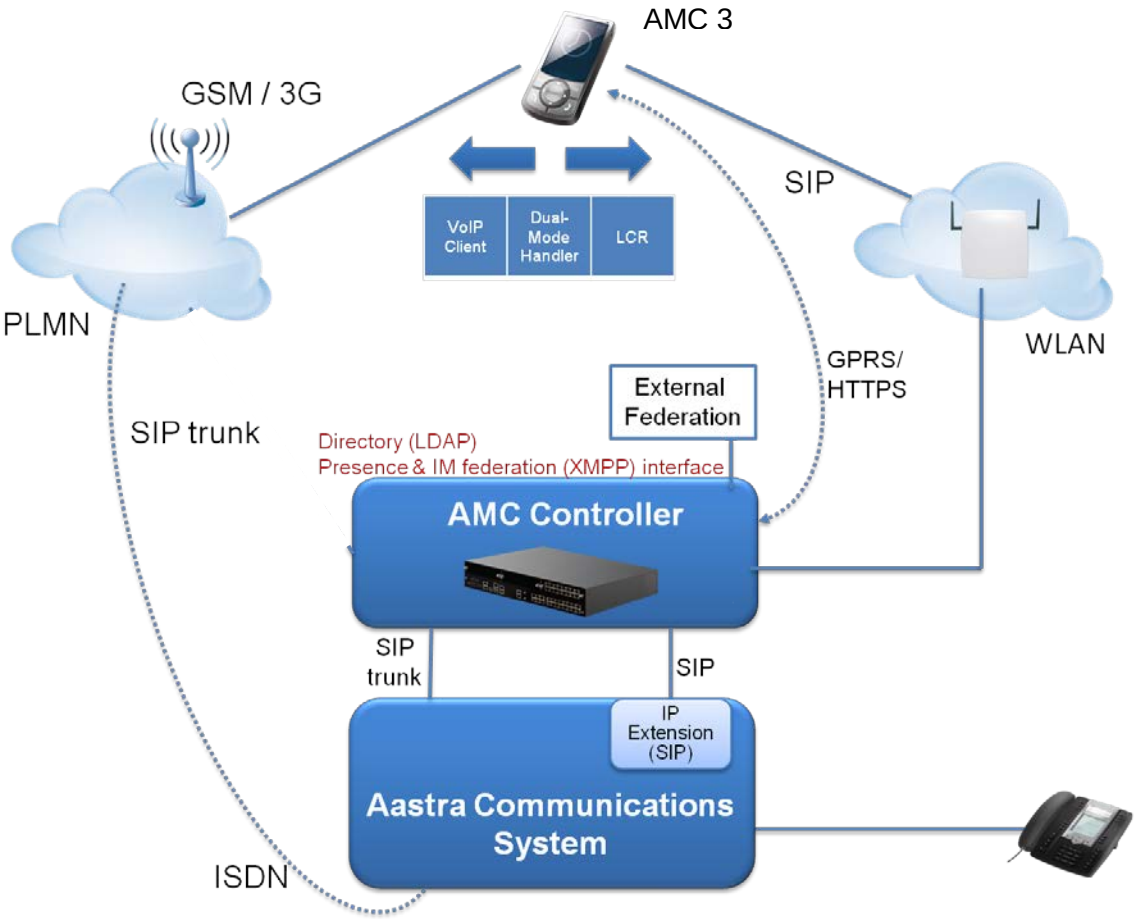

Figure 1: AMC Controller Solution

The AMC 3 solution consists of the following parts:

- The **AMCC** is the server for the mobile integration. It permits dual mode handover and Unified Communications features like Fixed-Mobile Convergence (FMC) capabilities for enterprise users. The dual-mode solution with handover capabilities (in both directions) is often referred to as a core part of the FMC concept. The mobile phones can be used like the user’s desk phone in the office (fixed or wireless). The AMC 3 user needs just one phone number to be reachable for customers and partners.
- The **AMCC Manager** is a web-based system used for configuration and administration of the AMCC. AMCC management software is part of the AMCC server and is accessible through any standard internet browser.
- The **AMC 3** is a mobile client application installed on a smartphone with 3G/GSM. The AMC 3 communicates with the AMCC using the SIP protocol. Voice communication is either SIP-based (WLAN) or traditional circuit switched-based (2G, 3G), depending on available networks.

3 AMC Controller 2.0

This section describes the AMC Controller, its components and requirements.

3.1 Architecture

The AMCC overview architecture is described in picture 2.

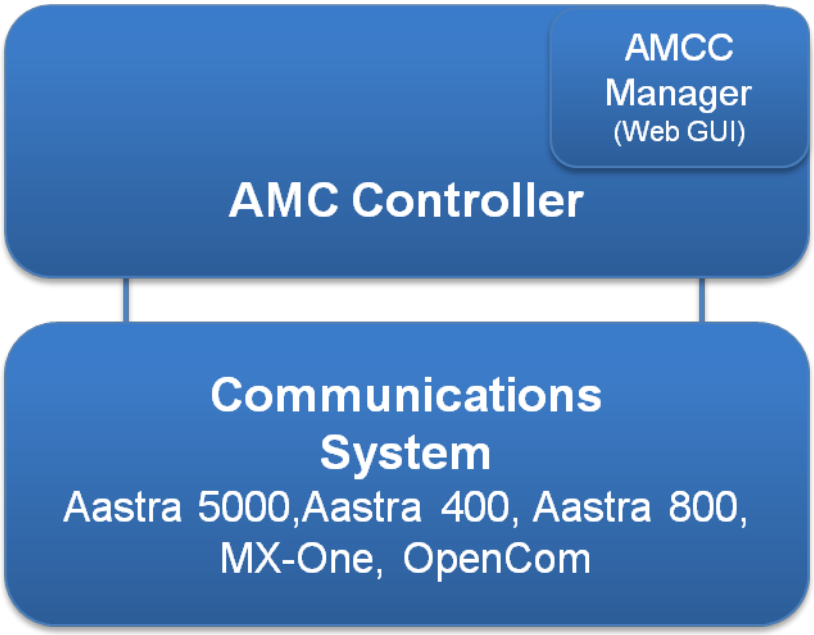

Figure 2: AMCC Architecture

The AMCC consists of the following:

- The **AMCC server engine** which is the core application responsible for providing some of the telephony related features like the seamless handover between 3G and WLAN, AMCC directory search, LCR, Instant Messaging (IM) and presence.
- The **AMCC manager** consists of a set of functions for system operations and management. It is used for server configuration and supports reporting functionalities for analysing the performance. For information about the deployment of the AMCC solution in an enterprise please refer to the according platform documentation.

3.2 AMCC Server

The AMCC server monitors the AMC 3 for any handover activity.

When the AMCC receives a request for handover from the AMC 3, the AMCC determines the type of vertical handover to be performed between the two mediums, VoIP and GSM. If a request for handover from VoIP to GSM is detected, the AMCC establishes a second call on the cellular interface for the same client. On Android the call is established by the AMC 3 on the device. Then the AMCC bridges the first call with the second call so that the A-party is now connected with the B-party using the GSM interface. Similarly, it can perform a seamless handover for the call from GSM to VoIP. Restrictions of

automated handover could be caused by mobile operating system and cause manual accepting of call on the device.

3.3 AMCC 2.0 Server Requirements WLAN

The WLAN should have the key performance indicators such as signal strength and low voice latency level to support Voice over IP communications. The AMCC communicates over the IP and MAC layer with the AMC dual mode application.

Please note that not every WLAN network offers the high quality of service which is required for VoIP. Sometimes you will find the term Wi-Fi, which is a registered trademark and not for general use of WLAN.

3.4 AMCC Capacity Options (SME)

AMCC has two capacity options:

- AMCC 130 installed for up to 150 AMC 3 users and max. 70 calls (no transcoding)
- AMCC 30 for up to 30 users with 10 simultaneous calls

4 AMCC Manager Features

The AMC Manager is a web-based configuration tool for the AMCC. The AMCC is a Linux-based application server supporting the administrator to perform all the necessary configurations via its web interface. It includes a basic system reporting. For more information regarding the AMCC Manager, see *User Guide AMC Controller*.

The AMCC Manager GUI provides one central point for the configuration of the AMCC via web browser, where the following actions are possible:

- Create, remove and edit the PBX data (IP access, call through number, etc.)
- Create, remove and edit the AMC extensions and SIP accounts
- View the current registration status of the dual mode users

System management:

- Activation of the changed system data
- System restart and shutdown
- System data backup and restore
- Trace and logging features
- System status reporting

5 AMC 3 Features

The AMC 3 supports the below listed features, dual-mode, directory search, encrypted VoIP, presence and IM.

The SIP compatibility of the AMC 3 allows the following functionalities (not all functions are available on all communications platforms):

AMC out-of-call-service

- Voice mail
- Call forward to any extension
- Message waiting indication
- Time group
- Call protect
- Diversion services: meeting, lunch, vacation...
- Corporate directory search

AMC In-call-service

- Fast forward number
- Take
- New Line / Enquiry
- Brokering / Toggling
- Conference
- Call Back
- Call Waiting
- Call Park

AMC Mobile LCR

- HTTPS call back & DTMF call through
- AMC travel SIM
- Dual mode (3G/GSM <-> WLAN/VoIP) automatic seamless handover[2]

AMC Unified Communications

- Instant Messaging
- Mobile Presence

AMC Encrypted VoIP (available on iPhone and Android in Q2 2013)

- TLS (signalling)
- SRTP (Media)

AMC Over the air (OTA) Provisioning and Licence Management

- Hosted Mobile LCR server

6 AMCC Key Features

- Dual mode two-way seamless handover between VoIP/WLAN and cellular networks, depending on device
- DTMF translation between in-band, out-of-band and SIP info format
- Network operator supported routing and AMC based routing
- Authentication of incoming calls (=trueCLIP)

[2] iPhone does not support automatic handover from WLAN to GSM, only from GSM to WLAN.

- Corporate directory search via LDAP
- IM & Presence via XMPP (external server required)
- Encrypted VoIP

7 Deployment

7.1 Installation and Configuration

Note: The AMCC has to be installed by trained and authorized system personnel in collaboration with local network administrator.

The AMCC software is delivered pre-installed on the AMCC. The latest software version is provided via the AMC Portal. For instructions on how to install the system, see the installation guidelines provided with the according PBX documentation. Once an AMCC is switched on, it is connected to the Ethernet, using the static IP addresses that were assigned during installation. For instructions on how to configure the system, see the "*User Guide AMC Controller"*.

7.2 Communication System Integration

The system administrator integrates the AMCC into the communications system by creating a SIP extension for each user in the communications system and configuring the SIP trunk in the communications system towards the AMCC.

7.3 AMC 3 Provisioning

The AMC 3 has to be provisioned on each AMC handset. This can be done through the AMC provisioning & licensing portal (http://amc.aastra.com/portal) via Over the Air Provisioning (OTA) or manually via USB or Bluetooth. For more information on how to install the AMCC application, see installation instructions.

8 Operation and Maintenance

All operation and maintenance tasks on the server are done using the web based AMCC Manager tool. Topics like fault management, configuration management, performance management information and certain reporting capability, along with backup and re-storage of configuration, are provided there.

The AMCC Manager is in charge of the following tasks with regard to the configuration of the server and extensions:

- System restart
- System shutdown
- System status
- System backup and re-storage

For more information on the AMCC manager, see the *"User Guide AMC Controller".*

9 Additional Features

9.1 High Availability

9.1.1 Linux HA-based Failover

AMCC supports Linux HA-based failover. There are two dual mode servers running the high availability application to act as a hot standby of each other. One of the servers providing dual mode service is called the primary server and the other one acting as its standby is called the backup server. The backup server is continuously sensing the status of the primary server ensuring its availability. In case the primary server goes down, the backup server takes over its role. This is called failover and it occurs within a few seconds.

The synchronization of the user data between two AMC Controllers is organised in a redundancy configuration. In such a configuration there are two appliances, one serving as a master and the other serving as slave. The slave will obtain its configuration from the master server. Therefore, this is not a real synchronization but rather having a master containing the configuration. The slave will keep a copy of the configuration ready to fill in if the master fails. This applies only to the FMC part of the configuration. Functions such as IP addressing etc. are considered separately. This automatically synchronized configuration includes all users, endpoints and registrations, numbering profiles, etc.

The synchronization is done by directly accessing the configuration database of the master server. All changes of users, endpoints or registrations will become effective immediately and will therefore also be scheduled for synchronization right after pressing "Save" in the AMCC Management Web GUI. In order to lower the network load, several changes are collected and then synchronized in one step. It can take up to 3 minutes until all changes have been properly synchronized to the slave device.

Configuration: The AMC Controller displays a "Database is currently not available" message on the pages TELEPHONY and FEATURES if it is run in slave-mode. The AMCC Database will not be available for changes and new data if database synchronization is ongoing and the AMC Controller is used in slave mode. All FMC services will be rendered by the master. Therefore, changes of registrations, user accounts, etc. can only be done on the master-AMC Controller. The data on the slave-AMC Controller will be synchronized (refreshed). If the master-AMC Controller fails, the slave-AMC Controller will take over. Only then, data modifications can be done on the (former) slave.

9.1.2 General Information

To configure both, master and slave, a network connection has to be set up. In theory a standard routed connection is enough, but since this feature is used in conjunction with VRRP, you need to have a connection supporting multicast requests, usually a switched connection.

9.2 AMC 3 Security

The AMCC offers services for enterprise telephony. The normal case is that it is placed in a closed network with end to end security. The AMCC offers SIP authentication based on message digest. An open source programme for filtering the by firewall offered tables, called **iptables**, is included and can be configured if needed. Usually, the enterprise has its own security measures and the AMCC does not play any critical role in enhancing the system or network security. Please see *“User Guide AMC Controller”* for more information.

9.2.1 AMC Controller Security Options

9.2.1.1 Password

On initial start up the administrator is forced to change the default password to a new password that has to fulfil certain complexity requirements in order to be accepted.

9.2.1.2 Direct Connection

The AMC Controller provides a pre configured firewall and runs on a hardened Linux operating system (OS). This allows to connect it directly to the internet without risk exposure of your internal network. The AMC Controller also has a built-in SBC component which provides even more protection.

9.2.1.3 Indirect Scenarios

There are some possible indirect setups for connecting the AMC Controller to the internet.

Choose the one that suits your system properties and/or requirements most.

9.2.1.4 With Intermediary DMZ

A demilitarized zone (DMZ) can be used to ensure higher protection of your internal system (and its information). “DMZ” describes a secure network area, which is separate from the internet and the local network. Normally, this is used for servers that have to be reachable from both the internal network and the internet (e.g. mail server, web server, etc.). In most cases a DMZ has official IP addresses.

9.2.1.5 Behind a Firewall with NAT and Port Forwarding

If the DMZ scenario is not an option, port forwarding and NAT behind a firewall is also supported. Of course a firewall can also be provided by the AMC Controller itself.

9.2.2 Security Guidelines

The AMC 3 dual mode handset requires corporate WLAN access. The service can be based on the unique SSID using wireless authentication and encryption using WPA / WPA2-PSK. A typical secure deployment scenario can be found on next page.

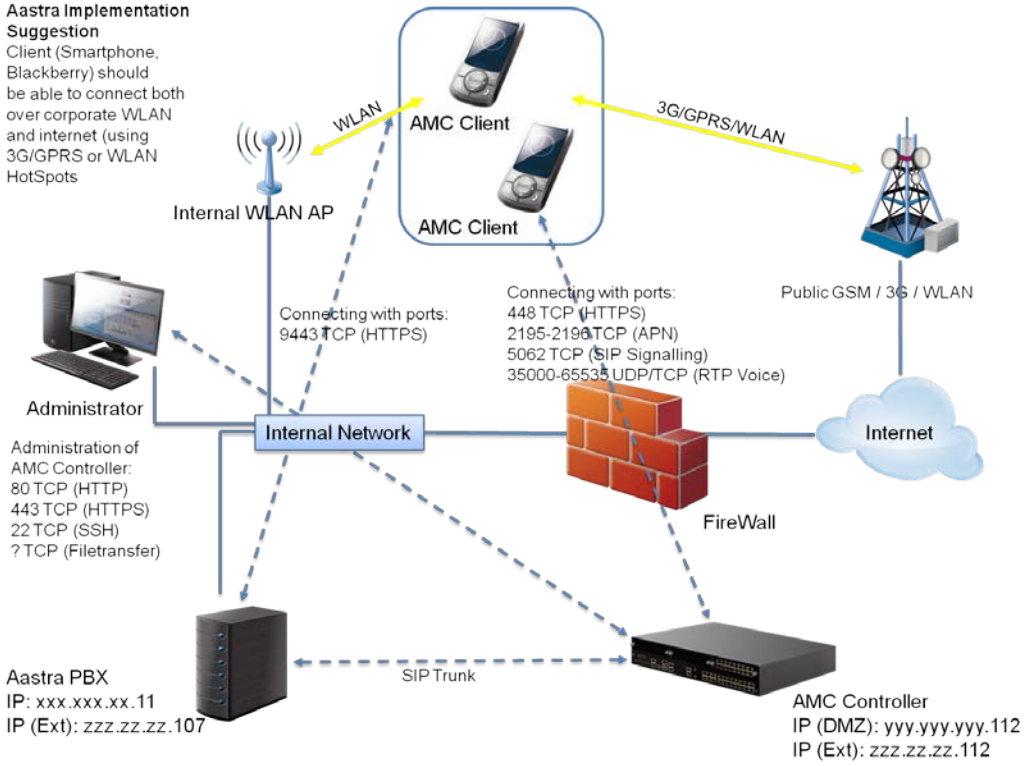

Figure 3: Voice over WLAN for Dual Mode Solution

9.3 AMCC Unified Communication Functions

With the AMCC UC functions the configured user accounts can get an HTTPS connection to the AMC Controller via their AMC. There are many different usage scenarios for this HTTPS connection. One of them is to enable users to access the complete company branch directory or the address book of just one department..

9.3.1 AMC Corporate Phonebook

The corporate phonebook server, to which you can configure a connection, has to be reachable via Lightweight Directory Access Protocol (LDAP). Commonly this will be an active directory server. The amount of information made available for the AMC via this feature of the AMC Controller depends on the information available on that server.

9.3.2 AMC Instant Message & Presence

XMPP is used for both, presence and instant messaging. For those features, the AMC Controller behaves very similarly to the SIP-telephony scenario. It will act as an XMPP client and connect to any standard XMPP server. XMPP is the most used Presence and Instant Messaging protocol and used for example by the Jabber or Openfire servers. There are both types, free and commercial, of servers available. You can also hook up to a Hosted Presence Network as for example Openfire and bring the full functionality of your account to the mobile phone. For a longer list of publicly available Instant Messaging servers, look at the XMPP website. There are also gateways available allowing connecting to non-XMPP Servers (e.g. SIMPLE) via the XMPP protocol. With this, the integration of any Presence / Instant messaging server should be possible. In order to use the XMPP functionalities you have to configure XMPP endpoints and XMPP users. As mentioned, this approach is very similar to the IP telephony approach. The concept of XMPP endpoints and XMPP users is essentially identical to the concept of SIP endpoints and SIP user accounts. For more information please read the AMCC Admin Guide.

© 2013 Aastra Deutschland GmbH. All rights reserved.
This document contains proprietary information, which is protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, or translated into another language, without the prior written consent of Aastra Deutschland GmbH, Berlin, Germany.
NOTICE The information in this document is subject to change without notice.
AASTRA MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Aastra shall not be liable for errors contained herein, neither for incidental nor for consequential damages in connection with the furnishing, performance, or use of these materials.

Aastra Deutschland GmbH Berlin, Germany